PERSEREC

Technical Report 14-03
September 2014

# Current Trends in Social Media and the Department of Defense's Social Media Policy

Andrée E. Rose
*Defense Personnel and Security Research Center*
*Defense Manpower Data Center*

Christina M. Hesse
Carollaine M. Garcia
*Northrop Grumman Technical Services*

Approved for Public Distribution: Distribution Unlimited
Defense Personnel and Security Research Center
Defense Manpower Data Center

**Technical Report 14-03** **September 2014**

# Current Trends in Social Media and the Department of Defense's Social Media Policy

Andrée E. Rose—Defense Personnel and Security Research Center/DMDC

Christina M. Hesse, Carollaine M. Garcia—Northrop Grumman Technical Services

Released by—Eric L. Lang

## BACKGROUND

Social media is dynamic. What we conceptualize today as social media will be different tomorrow. Advancing technological capabilities, including sophisticated mobile devices, have enabled social media's growth into almost every field of human activity. Social media's hallmark is to enable users to exchange data instantaneously with as many people as they choose.

Many Americans are in a state of near-constant connectivity. While this may increase productivity and create greater efficiencies with respect to how people manage their lives and do their work, it also introduces security and privacy risks that, if left unmitigated, could adversely impact national security, mission success, and personal safety. The Department of Defense (DoD) and the Services have developed policy and guidance to help personnel navigate the ever-changing dynamics, functions, and availability of social media.

## HIGHLIGHTS

Social media offers many benefits but it requires people to actively and effectively manage the information they share. This includes using good judgment about the type of information that is shared, properly implementing privacy settings, and staying up-to-date on social media platform modifications. Safety-related threats can emerge when social media management is inadequate. Sharing personal information or posting pictures of embarrassing or illegal behaviors online puts DoD personnel and their families at risk for exploitation by foreign intelligence services, terrorists, and criminals.

The pace at which social media evolves presents a challenge to policy-makers. DoD policy related to social media is sometimes outdated; nonetheless, it plays a critical role of informing the DoD community about safe and appropriate use. However, policy alone is not sufficient to protect DoD and its personnel from malicious actions. Social media guidance and training helps community members understand why the policy was implemented, and increases awareness about social media safety.

Defense Personnel and Security Research Center
Defense Manpower Data Center
400 Gigling Rd.
Seaside, CA 93955

# REPORT DOCUMENTATION PAGE

| | |
|---|---|
| **REPORT DOCUMENTATION PAGE** | **Form Approved**<br>**OMB No. 0704-0188** |

The public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing the burden, to Department of Defense, Washington Headquarters Services, Directorate for Information Operations and Reports (0704-0188), 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.

| | | |
|---|---|---|
| 1. REPORT DATE: 20140923 | 2. REPORT TYPE<br>Technical Report 14-03 | 3. DATES COVERED<br>May 2012-September 2014 |

| | |
|---|---|
| 4. Current Trends in Social Media and the Department of Defense's Social Media Policy | 5a. CONTRACT NUMBER: |
| | 5b. GRANT NUMBER: |
| | 5c. PROGRAM ELEMENT NUMBER: |
| 6. AUTHOR(S): Andrée E. Rose, Christina M. Hesse, Carollaine M. Garcia | 5d. PROJECT NUMBER: |
| | 5e. TASK NUMBER: |
| | 5f. WORK UNIT NUMBER: |
| 7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)<br>Defense Personnel and Security Research Center<br>Defense Manpower Data Center<br>400 Gigling Rd.<br>Seaside, CA 93955 | 8. PERFORMING ORGANIZATION REPORT NUMBER<br>PERSEREC: Technical Report 14-03 |
| 9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES) | 10. SPONSORING/MONITOR'S ACRONYM(S) |
| | 11. SPONSORING/MONITOR'S REPORT NUMBER(S): |

12. DISTRIBUTION/AVAILABILITY STATEMENT: (A) Distribution Unlimited

13. SUPPLEMENTARY NOTES:

ABSTRACT: Social media is dynamic. The only function that remains constant is its ability to connect people to one another. People's desire to communicate and stay connected with others has spawned new social media platforms that allow people to interact when buying groceries, real estate, music, books, etc. However, instead of sitting down at a computer to do this, the advancement of mobile devices and applications allow for these interactions to occur anytime and anywhere.

The pace at which social media evolves presents a challenge to policy-makers. DoD policy related to social media is sometimes outdated; nonetheless, it plays a critical role of informing the DoD community about safe and appropriate use. However, policy alone is not sufficient to protect DoD and its personnel from malicious actions. Social media guidance and training helps community members understand why the policy was implemented, and increases awareness about social media safety.

14. SUBJECT TERMS:

| | | | | | |
|---|---|---|---|---|---|
| 15. SECURITY CLASSIFICATION OF: UNCLASSIFIED | | | 16. LIMITATION OF ABSTRACT: | 17. NUMBER OF PAGES: 58 | 19a. NAME OF RESPONSIBLE PERSON: Eric L. Lang, Director |
| a. REPORT: UNCLASSIFIED | b. ABSTRACT: UNCLASSIFIED | c. THIS PAGE: UNCLASSIFIED | | | 19b. TELEPHONE NUMBER (Include area code): 831-583-4084 |

Standard Form 298 (Rev. 8/98)
Prescribed by ANSI td. Z39.18

# PREFACE

Since its inception, social media has continuously evolved through the creation of new platforms and mechanisms for people to communicate with friends and family, current and former colleagues, and people that they have shared interests with but have never met in person. While most of these interactions are positive, there are numerous instances where information-sharing created personal safety, operations security, and national security issues. The Defense Personnel and Security Research Center (PERSEREC) began studying social media usage among Federal Government employees in 2009. This effort builds on that work by identifying the changing dynamics of social media that introduce new and continued risks into the Department of Defense (DoD) community.

Eric L. Lang
Director, PERSEREC

# EXECUTIVE SUMMARY

Individuals conduct a vast amount of personal and professional activity online, and mobile devices such as smartphones allow users to have near-constant access to the Internet. Much of users' online activities involve social media, which includes "web-based tools, websites, applications, and media that connect users and allow them to engage in dialogue, share information, collaborate, and interact. Social media websites are oriented primarily to create a rich and engaging user experience. In social media, users add value to the content and data online; their interactions with the information (e.g., both collectively and individually) can significantly alter the experiences of subsequent users" (CIO Council, 2013).

NOTE: Blue text represents a hyperlink that enables you to jump to a term definition included in the Glossary. After clicking a link you can return to your previous location in the report by right-clicking on the page and select "Previous View" from the context menu.

The ability for individuals to instantly communicate with as many or as few people as they want has created challenges for the Department of Defense (DoD) and other federal agencies. In 2002 and 2003, war bloggers, usually military service personnel serving in Iraq and Afghanistan, were using the Internet to convey their wartime experiences with friends and family. Some bloggers were sharing mission-critical information that jeopardized operations security (OPSEC) (Associated Press, 2007). Consequently, DoD Components developed social media handbooks that provided online posting guidance to military service and civilian personnel. The goal of these policies is to encourage appropriate online behaviors, ensure posts do not reveal classified or controlled unclassified information, reinforce OPSEC, and prevent embarrassment to the DoD.

Despite this guidance, social media gaffes and abuses continue to occur. This report focuses on how social media has changed and identifies the ways in which sharing personal and mission-related information can potentially threaten national security, DoD's mission, and personal safety. This report does not address intentional disclosure of classified information but instead focuses on accidental, careless, and reckless social media mishaps committed by members of the DoD community for the purpose of identifying enhancements that need to be made to existing policies and guidance.

## METHODOLOGY

The information in this report is based on a qualitative study that included: (1) a literature review of peer-reviewed journal articles and news articles, (2) a review of the most popular social media websites' terms of service and privacy policies, (3) a review of DoD and service-level directives, instructions, and guidance, and (4) subject matter expert interviews.

## FINDINGS

### Trends in Social Media

The trends, methods, and uses for social media are constantly changing. Social media use among Americans significantly increased over the last decade from 8% in 2005 to 60% in 2013 (Brenner & Smith, 2013). It is the top Internet activity with Americans spending an average of 37 minutes per day on at least one social media platform and users spending 114 billion minutes a month on Facebook and 8 billion minutes a month on Instagram (Adler, 2014).

Social media engagement is no longer limited to the Internet via a desktop or laptop computer; more than half the time spent on social media is through smartphones and tablets (Adler, 2014). Users can access social networking profiles and platforms that include user-generated content through applications (apps) downloaded on their mobile phones. With the growing popularity of smartphones,[1] mobile app use has doubled from 2012 to 2013, and messaging apps have increased by 203% during this same time period (Khalaf, 2014).

Social media platforms are evolving to include multiple forms of communication. For example, image-sharing platforms, such as Instagram and Flickr, are integrating messaging capabilities, and traditional social media platforms, such as Facebook and Twitter, now provide opportunities for users to link social media accounts with other websites and applications. Additionally, the popularity of apps advertising self-destructing data (i.e., Snapchat and Confide) is growing as well as apps centered on anonymous sharing.

### Social Media Vulnerabilities

As social media evolves, it becomes increasingly integrated into everyday activities. Therefore, it is important for the DoD community to stay abreast of emerging social media platforms and potential security or privacy threats associated with those platforms. While social media is primarily a tool used for good, the ability to share information *en masse* can have negative real-world consequences. For example, military personnel can jeopardize OPSEC by posting seemingly harmless images, like a group of smiling Soldiers. Photos taken on a military installation or while in combat could inadvertently reveal location-based information through the metadata embedded in the images. Furthermore, personal information shared on social networks and blogs can be used to exploit login credentials (e.g., username, password, security question answers) for social media websites or other sensitive websites (e.g., banking, medical portals, shopping).

Social media promotes social interaction and encourages people to share information. Privacy settings provide the ability to control who sees what information, but they are dependent upon the social media platform's security.

[1] Twenty-two percent of the world's population owns a smartphone and 6% own a tablet (Heggestuen, 2013).

Privacy settings also offer no protection against the “trusted” friend who may copy or forward privately shared data. Users should be judicious when sharing information through social media in an effort to reduce their vulnerability to embarrassment and possible exploitation.

### DoD Social Media Policy and Guidance

The Services have developed handbooks, guides and messages that reference Department of Defense Instruction (DoDI) 8550.01, *DoD Internet Services and Internet-Based Capabilities* (2012). This is the primary governing document for DoD official and unofficial social media use. This report focuses on unofficial social media use. With respect to unofficial use, DoDI 8550.01 addresses appropriate standards of conduct, to include prohibitions on using personal social media accounts for official purposes and on disseminating non-public, sensitive, and classified information. It does not address mobile technology or apps. DoDI 8550.01 is currently undergoing an update and revision.

The Services’ social media handbooks and guides are thorough, relevant, and accurate, but not necessarily updated regularly. Furthermore, the extent to which these guides are read and understood is unknown.

## RECOMMENDATIONS

Based on the trends in social media, potential threats, and the current policies and resources issued by the DoD and the Services, the following actions are recommended:

(1) Conduct ongoing social media research because of the fast pace at which social media changes, so that policy-makers better understand how new and emerging capabilities might affect DoD and its personnel.

(2) Develop DoD-wide education and more clearly state training requirements that cover social media and mobile technologies.

(3) Develop and implement mandatory Defense Information Systems Agency’s (DISA) Information Assurance Support Environment training program related to the security risks and vulnerabilities of mobile apps.

(4) Update the DoD’s and the Services’ social media guidance on an annual or bi-annual basis so that it addresses the most current technologies and platforms. Furthermore, the Services should develop additional means for disseminating this guidance to ensure that Service members are aware of, and acting in compliance with, this guidance.

# TABLE OF CONTENTS

## LIST OF TABLES

## LIST OF FIGURES

## LIST OF TABLES IN APPENDICES

# INTRODUCTION

Social media refers to "web-based tools, websites, applications, and media that connect users and allow them to engage in dialogue, share information, collaborate, and interact. Social media websites are oriented primarily to create a rich and engaging user experience. In social media, users add value to the content and data online; their interactions with the information (e.g., both collectively and individually) can significantly alter the experiences of subsequent users" (CIO Council, 2013). A social media platform is the environment in which these interactions occur. Facebook, Twitter, YouTube, and Instagram are social media websites that allow users to create and/or share content, though each uses a different platform to format and deliver that content. Twitter allows users to post statements that are 140 characters in length, whereas Facebook limits the number of characters one can post to just over 63,000 (Buck, 2012). Similarly, Instagram allows users to post photographs, while YouTube specializes in user-generated videos.

NOTE: Blue text represents a hyperlink that enables you to jump to a term definition included in the Glossary. After clicking a link you can return to your previous location in the report by right-clicking on the page and select "Previous View" from the context menu.

The accessibility of social media on mobile technology, such as smartphones and tablets, allows users to have near-constant access to their social media accounts. To access any social media platform, a mobile device must have access to the Internet to navigate to the social media website or to download a specific mobile application (app). Mobile apps are software applications that allow users to connect with one another, play games independently or with others, access information (e.g., personal banking, classroom assignments, news articles, discussion forums) and generate content (e.g., capturing and posting photos and videos). Essentially, some mobile apps are social media platforms, while other mobile apps are designed to increase the efficiency and effectiveness by which users access and process information.

The ability for people to communicate with anyone at any time through traditional and mobile social media has been a lifeline for deployed military personnel. Instead of waiting for a letter to arrive or relying on phone calls to stay in contact, tools like Skype, a software application that allows users to have video conversations over the Internet, and Facebook, the world's largest social networking website, allow families to talk, message, exchange photos, and video conference as frequently as possible. Social media helps preserve the connectedness military personnel feel with their family and friends (Fitzpatrick, 2014; Leccese & Seligman, 2013). There are clear benefits to allowing military personnel to access and engage in social media but personnel need clear guidance on what is good and proper use because social media has presented many challenges to the Federal Government, and the Department of Defense (DoD) in particular. Military personnel, who share personal information on social media, even when they believe they are doing so anonymously, are vulnerable to exploitation by criminals and foreign intelligence services. Additionally, accidental disclosure of classified, controlled unclassified, mission-related and sensitive personal information in an online environment may allow terrorists, foreign governments, and other malicious actors to target Government and military personnel, as well as their families, in an effort to collect additional intelligence or seek retribution.

DoD should stay up-to-date on emerging trends in social media and mobile technology so that it can identify and possibly even forecast the potential threats that may arise when its personnel use this technology to share personal and professional information. As social media evolves and becomes more accessible, it is increasingly important to study and understand individuals' online behaviors that present a threat to national and personnel security (PERSEC). The purpose of this report is to describe the current state of social media, identify real-life accidental, careless, and reckless social media mishaps that are potential threats to the DoD, and review DoD's and the Services' social media policies and guidance to assess the extent to which these publications reflect current social media capabilities. This report does not address intentional disclosure of classified, controlled unclassified or mission-critical information via social media because the actions of active malicious insiders are better addressed by insider threat policy.

## BACKGROUND

The emergence and popularity of social media is fundamentally related to the Internet's transition from Web 1.0 to Web 2.0. Initially, Web 1.0 consisted of websites that supplied users with information but provided them with limited opportunities to comment on, add to, or revise posted material (O'Reilly & Battelle, 2009). When the stock market crashed in 2000, many Internet-based companies failed; however the companies that survived all used the Internet in a more dynamic way and rejected the static Web 1.0 design (O'Reilly & Battelle, 2009). These companies gave users the opportunity to publish their own content and interact with previously published online content (Wolcott, 2007). This evolution marked the transition from Web 1.0 to Web 2.0. This new type of online content posted by amateur Internet users, compared to strictly website owners, is referred to as user-generated content. Social media platforms all rely on this type of content.

Online behaviors using user-generated content can have both a positive and negative impact on users' physical lives. Professional networking websites may present users with new career opportunities, and dating websites are becoming an increasingly popular way for people to meet. However, online activities can have negative real-world effects for individuals as well. When these individuals are part of the DoD community, the consequences can be far reaching. For example, misuse of social media can harm national security (e.g., accidental release of classified, controlled unclassified, and mission-critical information in an online environment[2]), and create personal safety issues (e.g., identity theft).

It is important for the DoD community to be vigilant and to understand that it is each individual's responsibility to be smart about his/her use of social media. This requires increased awareness about the platforms that are being used and the information that is being shared. What might initially appear as benign information may be used to exploit the person who initially shared it. For these reasons, it is important for DoD, its military, civilian and contractor personnel, and their families, to be careful in their use of social media. There are hundreds of social media platforms and it can be difficult for a single person to stay up-to-date on best practices for using social media. The recommendations presented in this report ensure that guidance available to personnel and their family members is timely and relevant, and addresses both the platform and the content shared via social media.

[2] While information can be deleted from the location where it was originally posted, content may be copied by other social media users, and in many cases where the content is made publicly available, compiled by data aggregators.

# METHODOLOGY

The information in this report is based on a qualitative study that included (1) a literature review of peer-reviewed journal articles and news articles, (2) a review of the most popular social media websites' terms of service and privacy policies, (3) a review of DoD and Service-level directives, instructions, and guidance, and (4) subject matter expert (SME) interviews.

## LITERATURE REVIEW

For the purpose of this effort, articles that pertained to the development and evolution of social media, social media trends, work-place policy related to personal use of social media, and mishaps with social media were reviewed for relevant content. Sources consulted include peer-reviewed journals, military periodicals, organizational research, and news magazines that focus on digital culture and technology.

## DoD POLICY REVIEW

A comprehensive review of DoD and Service-level social media policy was conducted to identify existing social media policy and to determine where gaps, if any, exist across the DoD. This review also assessed consistency of social media policy across DoD and its Components, and examined the current efforts in place for informing the worldwide DoD audience about best practices in using social media. The DoD Social Media Hub ("the Hub") was consulted for this task. The Hub is a website designed to help DoD personnel use social media responsibly and effectively, both for official and unofficial purposes. It contains links to education and training, Terms of Service agreements, site registries, policies, and links to each of the Service's Social Media Portals.

## SME INTERVIEWS

Open-ended interviews with follow-on discussions were conducted with SMEs for the purposes of identifying trending websites and mobile applications, cyber behavior, policy and guidance, and current threats posed to organizations because of employee use and misuse of social media. SMEs consisted of the following individuals:

(1) Senior program manager from the International Association of Chiefs of Police.

(2) Proprietor from iNameCheck, a consulting company specializing in Internet intelligence.

(3) Director of Pew Research Center's Internet & American Life Project.

(4) Graduate students studying social media at the Massachusetts Institute of Technology's (MIT) Media Lab.

(5) Social media managers from the U.S. Army, U.S. Air Force, and U.S Marine Corps.

Interview questions included, but were not limited to:[3]

(1) How has social media changed from the early 2000s?

(2) What are current trends in social media usage?

(3) How will social media change?

(4) Have you, your constituents, or clients been negatively impacted by social media? If so, how? How did you address this issue(s)?

(5) How cognizant are people about online privacy?

(6) Besides privacy settings and nonengagement, are there other methods to protect online privacy?

[3] These were core questions that led to further discussion.

# FINDINGS

This section describes the findings from the literature review, privacy and terms of service policy reviews, DoD and Service social media policies, and SME interviews. The information is organized as follows: trends in social media and mobile apps, threats posed by social media, and an assessment of the usefulness (i.e., relevancy, thoroughness, and timeliness) of DoD's and military Services' social media policies.

## LITERATURE REVIEW

Social media use has increased over the last decade, growing from 8% of Americans having social media accounts in 2005 to 60% of Americans in 2013 (Brenner & Smith, 2013). It is the top Internet activity with Americans spending an average of 37 minutes per day on at least one social media platform and users within the United States spend 114 billion minutes a month on Facebook and 8 billion minutes a month on Instagram (Adler, 2014).

Social media is dynamic, and the most apparent trends for 2014 include the expansion of social media into almost all online domains, platform integration, increased use of mobile technology to engage in social media, anonymous sharing, and self-destructing data. Table 1 presents the most recent assessment of the different dimensions and functions of the social web (Solis & Thomas, 2013). These dimensions are not mutually exclusive, as several websites are multi-functional. For example, Twitter, a microblog, allows users to post text-based messages that are under 140 characters in length and it also allows users to post video clips that are under 7 seconds.

**Table 1**
**Dimensions of the Social Web**[4]

| Function | Definition | Examples |
|---|---|---|
| Social Networks | Focuses on facilitating relationships between people who might share interests, activities, or backgrounds. | • Facebook<br>• Google+ |
| Blogs & Microblogs | Blogs are self-published, discrete entries published in reverse chronological order. Microblogs allow users to share small elements of information such as short sentences, images, video, and links. | • Tumblr<br>• Twitter |
| Curation | Collecting, filtering, reviewing, and sometimes providing commentary on articles, images, and videos. Does not include creating new content. | • Pinterest |
| Location | Users submit location data for the purposes of interacting relative to their location. | • Foursquare |
| Reviews and ratings | Platforms that allow consumers to post reviews and opinions about services or products. | • Angie's List<br>• TripAdvisor |
| Social Streams | A stream of posts/updates from various social networks. (Fance, 2012). | • app.net |
| Social marketplace | An online community that uses social networks for the introduction, buying and selling of products, services, and resources | • Groupon<br>• Kickstarter |
| Social commerce | "Using social media to support social interactions for the purpose of assisting in the online buying and selling of products" (Marsden, 2009). | • Bazaarvoice<br>• livingsocial |
| Quantified self | Self-knowledge through tracking aspects of daily life (e.g., number of steps walked, heart rate, blood oxygen levels, etc.). | • Nike+ Running |
| Influence | A measurement of the extent to which people online are paying attention and responding to a user (Kellogg, 2013). | • Klout<br>• Kred |
| Social bookmarks | An online service that allows users to collect, annotate and share bookmarked websites. | • Evernote |
| Video | A video-sharing website that allows users to upload, share, view and comment on videos. | • Vimeo<br>• YouTube<br>• Twitter |
| Music | Audio services that transmit free and fee-based music via the Internet. | • Pandora |
| Events | Websites that allow users to find and promote events in local areas, such as festivals, concerts, rallies, etc. | • Zvents<br>• Plancast |
| Livecasting | Broadcasting real-time video feed to an audience accessing the video stream over the Internet. | • Ustream |
| Photos | Online photo-sharing platforms. | • Instagram<br>• Facebook |
| Documents | Hosting service that allows users to upload privately or publicly available documents. | • Docstoc<br>• Slideshare |
| Service | Platforms that allow users to search for or offer a variety of different services. | • Elance<br>• Crowdspring |

[4] Table derived from the Conversation Prism developed by Solis and Thomas (2013).

| Function | Definition | Examples |
|---|---|---|
| Business | Professional networking websites that allow users to connect with colleagues, search for jobs, recruit employees, etc. | • LinkedIn |
| Discussions and forums | Online bulletin boards that allow users to post and receive questions and messages. | • Google Groups |
| Wiki | A website, with no defined leader, that allows users to edit its content. | • Wikipedia |
| Enterprise | A social network for a specific company. Employees, customers, and suppliers may join to communicate with relevant users. | • Chatter<br>• Yammer |
| Nicheworking | A social network that allows users to connect with people who have the same interests or professional associations (Ronca, n.d.). | • Ravelry<br>• Classmates |
| Comments | Comment hosting services for websites and online communities | • Disqus |
| Q&A | Question and answer websites. Content is controlled by its users. | • Quora |
| Crowd wisdom | "The process of taking into account the collective opinion of a group of individuals" (Surowiecki, 2005). | • Buzzfeed<br>• Digg |

### Platform Integration

Some social media platforms allow users to link accounts to other social media platforms. For example, more than 2.5 million websites have integrated with Facebook (Rock, 2013). Known as social plugins, this tool allows users who are visiting various websites to interact with and post their current activity on Facebook. For instance, using Facebook's social plugins, one can "like"[5] another website or platform, "share"[6] an article, photo, or video found on another website or platform, or publicly comment on another website while using a Facebook account (Facebook.com, n.d.). This feature benefits Facebook in that it allows the company to engage more of its users' time and it provides additional data elements that it can collect and analyze for its own purposes.

As innovation progresses and new social media platforms are developed, larger technology-based companies purchase these startups to help ensure growth and survival. For instance, Facebook purchased the image-sharing service Instagram in 2012 and the mobile messaging app WhatsApp in 2014 (Rushe, 2014). These acquisitions, and others like it, suggest that social media companies are focused not only on expanding their own product, but also acquiring other social media platforms.

[5] A "like" is an action that can be made by a Facebook user. Instead of writing a comment for a message or a status update, a Facebook user can click the "Like" button as a quick way to show approval and share the message (Facebook, 2011).
[6] Sharing refers to when users post a link to another webpage on their social media account.

### Trends in Social Media Applications

Mobile applications (apps) first emerged in the 1980s and 1990s as tools that were not initially recognized as apps (e.g., games [e.g., Pong, Tetris, etc.], ring tone editors, calculators, and calendars). These tools came preloaded on cell phones but when smartphones were introduced there was a heightened interest in mobile apps because the operating systems allowed third party software to be installed (Clark, n.d.). [7]

Social media engagement is no longer limited to the Internet via a desktop or laptop computer; more than half the time spent on social media is through smartphones and tablets (Adler, 2014). According to the U.S. Digital Consumer Report by Nielsen (2014), Americans, on average, own four digital devices and two-thirds of Americans own smartphones. From 2012 to 2013, overall mobile use doubled and Figure 1 shows that the use of messaging and social apps increased by 203% (Khalaf, 2014). Furthermore, Juniper Research estimates that revenues from sales of mobile applications will approach $25 billion in 2014 (Clark, n.d.), suggesting that mobile technology and apps will continue to influence how Americans communicate, and are not fleeting trends.

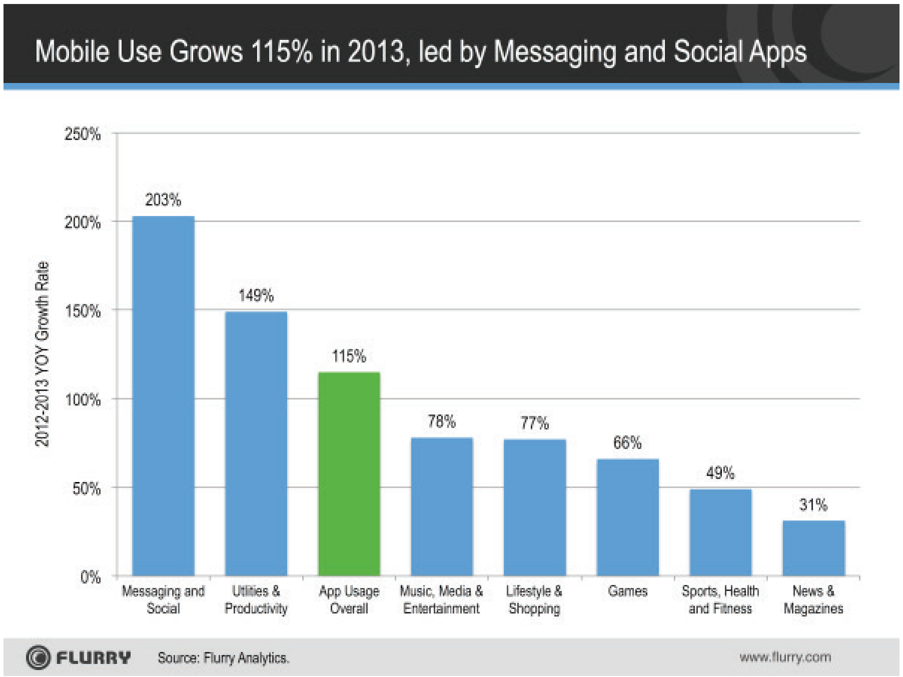


**Figure 1 Mobile Use Growth Increase**

Messaging apps are quickly replacing traditional mobile text messaging (Coldeway, 2014; Personal communication, graduate students at MIT Media Lab, July15, 2013)

[7] Third party software refers to software developed by an entity other than the original manufacturer or developer.

as a means of nonverbal communication. Instagram, a predominately photo-sharing website and app, recently introduced a private messaging service where users can share photos with up to 15 people who can comment on the photos in a group thread (Luckerson, 2013). By including this new feature, Instagram expanded from a strictly photo-sharing app to a messaging app. This type of expansion is emblematic of how social media evolves.

A development within messaging apps is the concept of self-destructing data. Users can send content and control how long the content is available for viewing by the receiving party. Snapchat, a popular messaging app, allows users to capture and send images and videos with added text to other Snapchat users, and can set up a time limit for how long the receiver has access to the information (i.e., self-destructing data).[8] Confide, a privacy-centric app marketed to executives and other types of professionals, is a text-based app where messages are revealed only one word at a time. As the receiver scrolls over the message, the first word disappears as the next one appears (Dellinger, 2014). Similar to SnapChat, users are lead to believe that the information they are sending will be destroyed and the content shared will not be linked back to them. However in 2014 SnapChat was sued by the Federal Trade Commission for deceiving users by marketing their app as one that could make messages "disappear forever," when in reality Snapchat developers could not guarantee their app would function as intended (Federal Trade Commission, 2014).

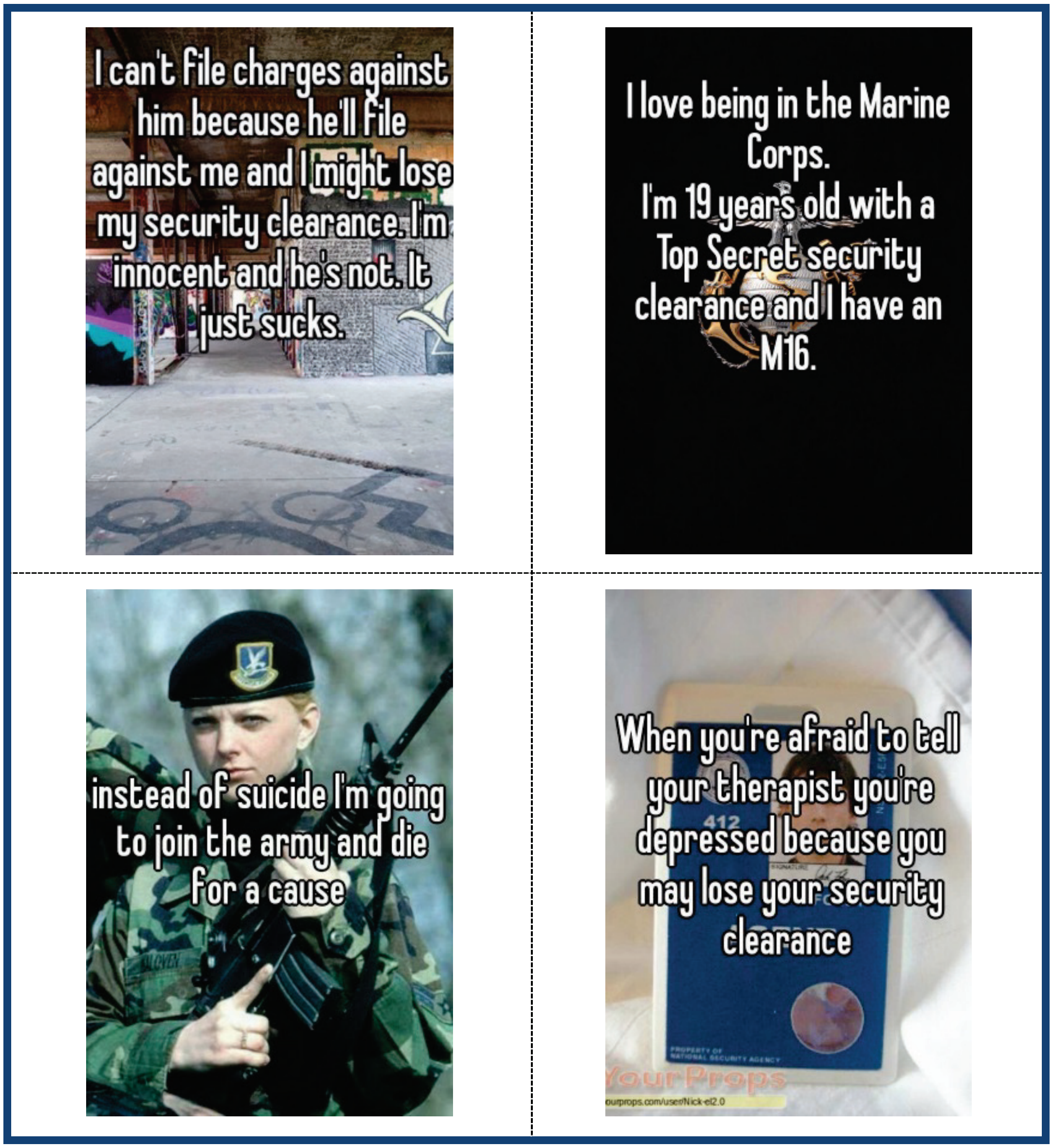
Another trending technology is anonymous sharing. The ability to share information without revealing one's identity has resonated with users, as evidenced by the number of users who have installed apps like Whisper and Secret on their mobile devices and the amount of funding raised by the two mobile app developers ($54 million and $8.6 million respectively) (Bessette, 2014).[9] Secret allows users to post anonymously; however, it connects users' accounts to their phone contacts and shares posts from primary and secondary connections (i.e., friends of friends).[10] Whisper allows its users to post brief messages (i.e., secrets) in the form of "text superimposed on a picture" and "users can respond to secrets by sending either a public or private message (Gannes, 2013)." See Figure 2. This anonymity encourages spontaneous expression, leading to what some would call an honest confessional.[11]

[8] In 2014, Snapchat introduced live chat and video conversation capabilities, and the messages sent during a live chat are deleted once the user exits the conversation (Datoo, 2014). This development further supports the finding that social media apps are blending platforms.

[9] Google Play Store is over 1.1million.

[10] Secret is not the only mobile app that requires users to connect their account to their email or phone contacts, an emerging trend in social media apps. Similarly, some mobile apps, like the messaging app Confide, require users to connect their account to their Facebook profile.

[11] Less than 3 years old, Whisper has referred more than 40,000 users to suicide hotlines (Bowles, 2014), and some of these users identify as current or former military personnel (Zimmerman, 2014). In response to the overwhelming number of subjects who post thoughts about depression, anxiety, and suicide ideation, Whisper launched the nonprofit website, *YourVoice.* Tailored for college-age users, this website hosts anonymous, user-submitted content that describe how they came out on the other side of depression.



I can't file charges against him because he'll file against me and I might lose my security clearance. I'm innocent and he's not. It just sucks.

I love being in the Marine Corps.
I'm 19 years old with a Top Secret security clearance and I have an M16.

instead of suicide I'm going to join the army and die for a cause

When you're afraid to tell your therapist you're depressed because you may lose your security clearance

**Figure 2 Anonymous Posts from Whisper (Stock Images Available on the App)**

## SOCIAL MEDIA VULNERABILITIES

While there are many benefits of social media engagement, sharing personal information in this environment can make people, and sometimes the organizations they work for, vulnerable to malicious actors. Vulnerabilities may be exploited when the following occurs:

(1) Social media users do not understand the full functionality of the platforms or devices they use, and accidentally release personal or work-related information to the public that can later be used for criminal activity.

(2) Adversaries use fraudulent social networking accounts to "friend" or "connect" with people who are targeted for intelligence collection.

(3) Social media users anonymously share explicit or sensitive personal information without realizing they may have provided an Internet Protocol address[12], phone number, email address, or some other breadcrumb embedded in the file (i.e., metadata) or visible in the image (e.g., a name on a uniform, a familiar background, etc.), which creates an opportunity for blackmail, coercion, or harm to personal safety.

(4) People share explicit or sensitive personal information using a self-destructing data app without recognizing that friends may use counter-apps to preserve their data for the purposes of ridiculing, embarrassing, or even blackmailing the sender.

(5) Criminals use publicly available personal information to physically, emotionally, or financially harm others.

Aside from eschewing all forms of social media, the most effective way to mitigate these vulnerabilities is to use good judgment when sharing information. Good judgment includes being smart about the devices and platforms that are used, limiting the type and amount of personal information that is shared, and implementing the most restrictive privacy settings with the understanding that even these are fallible.

Privacy settings restrict access to social networking profiles and allow users to limit what information other users can see. However, a recent report found that these settings do not completely insulate users from hostile actors (Rainie, Kiesler, Kang, & Madden, 2013). Twenty-one percent of Internet users reported an email or social networking profile was hacked and 11% indicated that important personal information, such as their social security number, was stolen from the Internet. Additionally, a recent study found that more than 20 social media websites leaked private user information to third-party tracking sites (Guadin, 2010).

Furthermore, a primary cause of accidental disclosure of information on social networks and other social media outlets is poor privacy management. Users often do not take time to read privacy policies and properly implement these settings unless they have been negatively impacted by the release of information online (L. Rainie [Director of Pew Research Center's Internet & American Life Project], personal communication, September 17, 2013). A February 2012 study released by the Pew Research Center's Internet & American Life Project found that almost 60% of social networking website users implemented privacy settings to restrict access to their profiles, but 16% of these users indicated that it was somewhat difficult to manage their privacy settings, and 2% indicated it was very difficult to use privacy

[12] Multiple websites offer free and fee-based services that identify the location of an Internet Protocol address (e.g., infosniper.net, ip2location.com, etc.)

settings (Madden, 2012).  Another study found that social networking users' intentions to restrict access to their social networking data did not align with the actions they took to restrict access. Furthermore, many of these users were either unwilling or unable to address these privacy lapses (Madejski, Johnson, & Bellovin, 2012). Consequently, misapplying privacy settings can cause widespread dissemination of information that was intended for a specific audience.

In some instances users may purposely choose not to implement privacy settings because there is value in disclosing personal information in a public domain (L. Rainie, personal communication, September 17, 2013). Job seekers may share their name, location, work history, and educational achievements on professional social networks like LinkedIn to meet job recruiters. In other cases, research has found that people who score high on narcissism, which is an inflated sense of worth and a need for admiration, tend to overshare and use less restrictive privacy settings on social networking websites (Utz & Kramer, 2009; Kramer & Haferkamp, 2011). For these users, the immediate advantages of sharing personal information overpower long-term vulnerabilities. These vulnerabilities may include intelligence collection, blackmail and coercion, and threats to personal safety.

### Intelligence Collection

According to the National Security Agency (NSA), "Intelligence is the product resulting from the collection, collation, evaluation, analysis, integration, and interpretation of collected information" (NSA, n.d.). The collection of information is an active phase that requires an adversary to seek out specific individuals, agencies, websites, government and commercial records, etc., for the purposes of identifying and retrieving valuable information. This information will then be used to retrieve higher value information that may ultimately benefit the adversary and harm the United States.

Increasingly, terrorist organizations and foreign governments are turning to social media as a source of information about DoD personnel, capabilities, and activities (Department of Homeland Security, 2010; Social Media Today, 2013; Shephard, 2013). A 2009 post on a jihadist website called for its operatives to collect intelligence about U.S. warships and its personnel and their families in the Gulf of Aden (Ewing, 2010):

> …with Allah's help, all American vessels in the seas and oceans, including aircraft carriers, submarines, and all naval military equipment deployed here and there that is within range of Al-Qaeda's fire, will be destroyed…To this end, information on every U.S. naval unit – and only U.S. [units]!! – should be quietly gathered [as follows:] [the vessel's name, the missions it is assigned; its current location, including notation of the spot in accordance with maritime standards; the advantages of this naval unit; the number of U.S. troops on board, including if possible their ranks and what state they

> are from, their family situation, and where their family members (wife and children) live…monitor every website used by the personnel on these ships, and attempt to discover what is in these contacts…

Furthermore, terrorist organizations such as Hezbollah and Al-Qaeda have used fraudulent social networking profiles[13] to recruit and collect intelligence from Service members' accounts, and group discussions (Likmeta, 2014; Doll, 2012). In 2007, an attack on four AH-64 Apache attack helicopters in Afghanistan was directly attributed to Soldiers who posted pictures of the helicopters on their social media accounts (Zhang, 2012). Meta-data, stored within the digital pictures, provided insurgents with the precise location of the helicopters. The Army openly discussed the incident in 2012 and issued guidance recommending that Soldiers disable geotagging features on phones and adjust social media privacy settings to prevent sharing location-based information with potential adversaries (Rodewig, 2012).

Foreign governments are also suspected of using fake profiles to collect information. In 2012, several individuals associated with the North Atlantic Treaty Organization (NATO) accepted a Facebook friend request from U.S. Navy Chief Admiral James Stavridis, the Supreme Allied Commander of NATO. However, this was a fraudulent Facebook profile and Chinese government agents are suspected of creating it to gather intelligence. Exactly how much intelligence and the importance of the information remain uncertain (Jones, 2012; Lister, 2012).

Similarly, between 2011 and 2014, Iranian hackers participated in an elaborate digital attack against U.S. military personnel, members of Congress, diplomats, lobbyists, and Washington-based journalists (Koren, 2014). This social-engineering campaign incorporated dozens of fake social media accounts on various platforms, including Facebook, Twitter, and LinkedIn. If users clicked on a link sent via these fake accounts, malware was sent to their computer. In addition, the campaign involved a fake news website. It is currently unknown what information was stolen (Koren, 2014).

### Blackmail and Coercion

Blackmail presents a real and serious threat to the DoD. Advancing technology makes it easier to collect evidence of illicit or illegal behavior, and it also allows for this collection to occur on a larger number of subjects. Furthermore, people may be surveilled when they are in the infancy of their careers, and incriminating information may be digitally saved until they are in sensitive and powerful positions (Fingleton, 2012). Tumblr, a mini-blogging service, has several publicly available webpages that are dedicated to posting sexually explicit images of active duty military personnel (e.g., *Major Dad's Military Nudes, Military Nudes, Military Men*

[13] There is evidence that terrorist groups created fraudulent Facebook profiles posing as attractive women with the intention of "friending" military service personnel to spy on them (The Week, 2012).

*Collection, Military Girls in Various Stages of Undress,* etc.).[14] Service members are encouraged to send their explicit images, sometimes while in their Service uniforms, via text message or email to the owners of these pages, who then re-post the images.[15] Images are usually posted anonymously but many times identifiable features such as their face, name on their uniform, and tattoos are visible in the image. This may place Service members at risk for blackmail or coercion because the owners of these Tumblr accounts have their personal information (e.g., phone number or email address associated with the submitting party and any other personal information submitted with the image). In addition, these posts also negatively affect the public image of the Armed Forces.

Similarly, self-destructing messaging apps encourage users to capture images, video, and text that they would otherwise not release to the public. Users are led to believe that the information they are sending will be destroyed and the content shared will not be linked back to them. However, the development of counter-apps has put self-destructing app users at risk. The app SnapCapture[16] was designed to circumvent time limits. Consequently, users' personal data could be: (1) shared with a larger audience causing embarrassment and shame, (2) used against them through blackmail or coercion, or (3) shared with law enforcement. While there have been no indications that DoD employees have been counter-app victims or perpetrators, there have been numerous instances where members of the general public have suffered serious repercussions from these types of apps.[17]

### Personal Safety

When users disclose personally identifiable information (PII) on the Internet, they may be exposing their information to hackers and identity thieves. A hacker can take control of users' social media accounts or create fraudulent social media accounts using stolen PII.  In turn, hackers can gain access to other users' PII who are connected to the original user on social media. Furthermore, criminals can use PII and other personal information (e.g., answers to possible security questions such as name of dog, name of childhood best friend, or name of first school) to

[14] Some images appear to have been taken at military installations, possibly revealing location-based information.

[15] It should be noted that in some cases images may have been submitted by jealous ex-lovers or others who are attempting to embarrass the subject of the photos.

[16] Google removed SnapCapture from the app store in May 2014 due to a violation of the developer agreement; however, users who had already downloaded the app may still use it.

[17] In December 2013, an Ohio University student was charged with four felonies for engaging in a Snapchat sex extortion scam. The student pretended to be a woman when he flirted with other male college students on Snapchat. He sent naked photos of a woman in exchange for naked photos of the men. "The 'female' then alleges that unless he engages in sexual conduct with a third party male, that she's going to leave it up and add all of his friends to this post…So she extorts him to engage in sexual conduct with a male, in order to take these photos down." When the perpetrator met the other male student, he claimed to be blackmailed by the same woman. Those sex acts were also recorded, reportedly, to continue blackmailing the victim." (Westerholm, 2013).

access bank accounts and credit card information. Information shared online can also reveal behavioral patterns that can be used to stalk individuals.

Criminals may also be using "stalker" apps to learn more about the people they pursue (see Table 2). Name Tag, Name Tag, a facial recognition app, can be used to match a picture to an established social media profile or other online content associated with a specific person; as an example, a Name Tag user can take a picture of someone on the street and the app will attempt to match the face to publicly available content (e.g., social media profiles such as Facebook, dating sites such as Match.com, and possibly even criminal or sex offender registries). The app queries publicly available information only, making social networks' privacy settings all the more important. Users may also copy online images (e.g., from a dating website) and conduct a search (Vaas, 2014).

**Table 2**
**Applications that can be Used to Track Other Social Media Users or Engage in Discreet Information Collection**

| Application | Purpose |
|---|---|
| SWARM | Allows users to find their social media friends' current locations. |
| Stalker | Allows a smartphone's camera to operate in stealth mode. The flash is turned off and the shutter is muted. The screen looks like a text messaging screen instead of revealing the image that is about to be taken or has been captured. |
| Breakup | Allows users to set up an alert whenever specific Facebook friends change their relationship status. |
| Girls Around Me | "This foursquare-based tool helps you see where nearby girls are checking in, and shows you what they look like and how to get in touch! You can also search for guys or see who's hanging out at a particular place. Girls Around Me scans your surroundings and helps you find out where girls or guys are hanging out. You can also see the ratio of girls to guys in different places around you." (girlsaround.me, n.d.) |
| Creepy | Users can collect location data from friends' social media platforms and pinpoints this data on a map. It quickly and easily allows users to identify where their friends frequent, or may currently be located. |

Source: Table is derived from the article *9 Creepy Apps to Watch out for: SWARM, Stalker, Crush, Wingman, Name Tag, Breakup, Girls Around Me* by Alter and Rivas (2014).

## POLICY REVIEW: DoD SOCIAL MEDIA POLICY AND GUIDANCE

A 2014 survey of 110 private businesses found that most employers believe that employee misuse of social media will become more problematic in the future. More than half of the businesses surveyed had to address the misuse of social media within the last year, and of those, 71% initiated negative employment actions. Almost 80% of these businesses have a social media policy but only 53% updated their policy within the last year. Furthermore, fewer than 50% trained their employees to use social media responsibly (Proskauer Rose LLP, 2014). Although these results were gathered about employees in private industry, they should apply equally to Government employees. These findings suggest that policy and training are key resources to reducing social media missteps and misuse.

Social media policy is important for informing and educating DoD personnel about safe and appropriate social media usage. Furthermore, social media policy directed at military service personnel should draw upon other relevant DoD policies and the Uniformed Code of Military Justice (UCMJ) that address prohibited political activities (DoD Directive [DoDD] 1344.10,*Political activities by members of the Armed Forces,* 2008), prohibited protest activities (DoDD 1325.6, *Handling dissident and protest activities among members of the Armed Forces,* 2012), disrespect toward a superior commissioned officer (UCMJ Article 89), and making negative comments about the United States President, Vice President, and other United States political officeholders (UCMJ Article 88). Personnel should be reminded that online behavior is real behavior; DoD and service-specific policies that prohibit or restrict certain activities pertain to both the online and physical environments.

Information and education can protect personnel, their families, and DoD assets from many types of malicious action. This section details the policies that DoD and the Services have implemented. Policies specifically addressing personal use of social media are discussed in Table 3.

**Table 3**
**Instructions, Guidance, and Memoranda Pertaining to Personnel's Unofficial Use of Social Media**

| Instructions, Guidance, and Memoranda Pertaining to Social Media | | |
|---|---|---|
| **Publication** | **Description** | **Issue Date** |
| **DoD** | | |
| DoDI 8550.01 DoD Internet Services & Internet-Based Capabilities | Defines responsible and effective use of Internet-based capabilities, including social networking sites. | September 11, 2012, updated version forthcoming |
| Social Media Hub[18] | A DoD website dedicated to social media education and training. | No release date |
| **U.S. Army** | | |
| The United States Army Social Media Handbook Version 3.1 | Information for both official and unofficial use of social media. Topics: safe social networking, operational security, tips,[19] and case studies. | January 2013 |
| Social Media Roundup: Social Media Headlines to Watch for in 2013 | A Slideshare presentation that discusses Google+, the growth of mobile technology, and new social media platforms (e.g., Snapchat). | January 9, 2013 |
| **U.S. Navy** | | |
| ALNAV 057/10 Internet-based Capabilities Guidance – Unofficial Internet Posts | "Post accurate and appropriate information that does not compromise mission security or success." Do not post sensitive information, guard PII, be mindful of online associates, and use privacy settings. | August 19, 2010 |
| Navy Command Leadership Social Media Handbook | Describes policy and provides guidelines for personal, as well as guidelines for official command social media sites. | November 16, 2012 |
| U.S. Navy Social Media: Facebook News Feed | Discusses how Facebook uses user feedback and interaction to determine the content that is shown in a users' main page. | August 12, 2013 |
| **U.S. Air Force** | | |
| Navigating the Social Network: The Air Force Guide to Effective Social Media Use | Provides social media guidance for Airmen and family, identifies Air Force policies, and notes security and privacy issues. | March 2012 |
| Air Force Social Media Guide | Defines social media terms, provides guidance for Airmen and families, and identifies trends in social media and | June 1, 2013 |

[18] Articles range in date from 2010 to 2013.

[19] Tips for Soldiers, Army Families and Army Personnel include Army guidelines found on SlideShare that provide the following guidance and expectations for soldiers: a reminder to follow the Uniform Code of Military Justice when posting, use caution when posting sensitive information, avoid geotagged information and photos, uphold Operations Security (OPSEC), and review privacy settings.

| Instructions, Guidance, and Memoranda Pertaining to Social Media | | |
|---|---|---|
| **Publication** | **Description** | **Issue Date** |
| | safety tips for posting online. | |
| **United States Marine Corps (USMC)**[20] | | |
| Marine Administrative Message (MARADMIN) 181/10 Responsible and Effective Use of Internet-based Capabilities | Defines responsible and effective use of Internet-based capabilities, including social networking sites. [Personnel should] continue to "defend against malicious activity affecting DoD networks…" (DTM 09-026). | March 29, 2010 |
| MARADMIN 365/10 Social Media Guidance - Unofficial Internet Posts | "Post accurate and appropriate information that does not compromise mission security or success." Do not post sensitive information, guard PII, be mindful of online associates, and use privacy settings. | June 30, 2010 |
| The Social Corps: The U.S.M.C. Social Media Principles | Provides guidance for Marines and families[21], and creates awareness on OPSEC, privacy settings, and security. | January 2012 |

In an effort to help its community navigate social media, the Office of the DoD Chief Information Officer (DoD CIO) developed the Social Media Hub ("the Hub"). The Hub was designed to help users engage with social media and other Internet resources safely and securely. It provides links to DoD and federal policies that are relevant to personal and professional use of social media, and it provides education and training resources for social media use. In addition, the DoD CIO participates in milBook Webmasters and social media groups in order to provide additional guidance, tips, and advice to the Services regarding social media use (DoD CIO, personal communication, July 14, 2014).

The Defense Information Systems Agency's (DISA) Information Assurance Support Environment is another robust resource. DISA's online training catalog provides computer-based training on using smartphones and tablets[22] and on social networking.[23] Both types of training provide overviews of the security risks and vulnerabilities associated with using these devices and platforms, and tips for making informed decisions on social networking activities.[24] However, these trainings require revisions and updates. Aside from The Hub and DISA's online training catalog, DoD offers the Services minimal guidance on social media policies

[20] Though there are no social media-related presentations, the Marine Corps' website has a series of linked documents that discuss privacy settings and security issues, the permanence of online content, safety of extra information unwittingly provided in pictures taken, and a reminder not to post PII or sensitive information online.

[21] Social media and families: Be careful about posting personal information (e.g., military photographs, exact time/location of deployment); avoid posting sensitive information; Operational Security.

[22] Released March 2013

[23] Released March 2011

[24] http://iase.disa.mil/eta/online-catalog.html#iaatraining

and safe practices (T. Schusler [Air Force Chief of Social Media], personal communication, June 11, 2014).

Because of frequent changes in social media, it is challenging to keep policies and guidance up to date. The Services do not have published regulations or instructions that address personal or unofficial social media use. Instead, the Services developed handbooks, guides, and messages that reference Department of Defense Instruction (DoDI) 8550.01, *DoD Internet Services and Internet-Based Capabilities* (2012). This is the primary governing document for DoD official and unofficial social media use[25]. With respect to unofficial use, DoDI 8550.01 addresses appropriate standards of conduct to include prohibitions on using personal social media accounts for official purposes and on disseminating non-public, sensitive, and classified information. An updated version of DoDI 8550.01 is forthcoming (T. Davis [Deputy Director Information Management, Office of the DoD Chief Information Officer], personal communication, July 14, 2014).

The social media handbooks and guides developed by the Services identify possible threats to personal safety and national security, and include suggestions for using social media wisely. These handbooks and guides are thorough, relevant, and accurate, but should be updated more frequently in an effort to stay current with emerging media. The pace at which social media platforms evolve requires near-constant updates on OPSEC and personal security. However, it is challenging to update policy as quickly as social media changes because of the lengthy publication process (B. Brown [U.S. Army Social Media Manager], personal communication, June 10, 2014). The official websites for the Army, Marine Corps, and Air Force provide links to social media policy and guidelines, including a link to their respective social media handbooks.

The Services' social media managers[26] have attempted to fill the gaps between the annual publication of their handbooks by using Slideshare, a slide hosting service, to release publicly available guidance on the latest trends in social media and mobile apps. Army Commanders (Commanding Officers, or COs) are encouraged to download social media slideshows posted on Slideshare and edit the slideshow to tailor it for their unit (B. Brown [U.S. Army Social Media Manager], personal communication, June 10, 2014). The purpose of this is to empower COs to monitor their unit's social media activity. Because there is no Army-wide social media policy, COs are also encouraged to create their own guidance using a template provided on Slideshare, thereby generating a way to enforce safe social media use. The Air Force would like to develop a similar approach for distributing social media information (T. Schusler [Air Force Chief of Social Media], personal communication, June 11, 2014). For the Marine Corps, there is informal training during boot camp and officer candidate school addressing how to represent the Marine Corps online.

[25] This report focuses specifically on unofficial social media use.

[26] Because of personnel changes, the authors were unable to discuss social media policy and strategies with the Deputy Director of DoD Social Media at the Defense Media Activity.

The Marine Corps Social Media Chief suggested that formal training on safe social media use prior to Marines joining the fleet would be beneficial (M. Fayloga [Staff Sgt., Marine Corps Social Media Chief], personal communication, June 24, 2014).

Similarly, the Army and Navy use Facebook and other social media resources to help raise awareness about social media and OPSEC issues. The Facebook page *Naval Operations Security* provides timely and relevant articles on safety concerns associated with social media and mobile technology while also providing OPSEC tips. For example, the page advises users to “be vigilant with privacy settings so you’re not allowing apps you don’t even use access to your private content” (a reference to stalker apps). However, the Navy’s *Operations Security* Facebook page only has 12,730 “likes,” indicating that only a fraction of Navy personnel and their family members are receiving regular safety updates via their Facebook newsfeed.

# DISCUSSION

This report summarizes recent trends in social media, including messaging and social mobile apps, and assesses the extent to which DoD and the Services address potential threats to national security, OPSEC, and personal safety through policy and guidance.

As social media use increases, the variety of platforms available has become more diverse. These platforms are evolving in a way that makes categorization and differentiation difficult because platforms are incorporating various types of elements, like messaging and image-sharing services, and are providing users with more than one way to share information. Furthermore, the social media platforms of today are not the platforms of tomorrow.

Specifically, the growth of smartphone use and the presence and use of social media apps is increasing. Messaging apps are replacing other forms of nonverbal communication, and apps advertising self-destructing content are growing in popularity. Similarly, anonymous sharing is becoming more and more popular, and as a result, users are sharing more information online because they believe it cannot be linked back to them.

Social media can be extremely beneficial in its ability to connect individuals across states and countries, and mobile apps provide users with near-constant access. However, inadvertent or deliberate misuse of social media by Service members can potentially have adverse consequences to the national security interests of the United States. Users make themselves more vulnerable with poor privacy management, and when those users are part of the DoD community they can be targeted for intelligence collection by terrorist organizations, foreign countries, and other malicious actors. DoD personnel can unintentionally reveal classified, controlled unclassified, and mission-critical information online. Even seemingly innocuous images can reveal location-based information through the metadata embedded in the digital image. Furthermore, if users share private and potentially damaging information online (i.e., explicit images) they increase their vulnerability to blackmail and coercion. This, in addition to potential hacking schemes, identity theft, and stalking, threaten users' personal safety.

Given the pervasiveness of social media and mobile technology, the Services have done an exceptional job providing guidance on advancing platforms and capabilities. However, the extent to which this guidance is accessed, read, and understood is unknown. DoD must ensure social media policies and guidance are relevant and timely, and require social media training for DoD civilians, contractors, and military personnel.

By analyzing the trends in social media, it is evident that online and mobile communication is constantly evolving and becoming increasingly popular. Because of its dynamic state, it can be challenging to predict potential threats generated from social media use and to develop appropriate and current policies. The best way to prepare for threats from social media is to be proactive.

# RECOMMENDATIONS[27]

Based on trends in social media, potential threats, and the current policies and resources issued by the DoD and the Services, the following actions are recommended:

(1) Conduct ongoing social media research because of the fast pace at which social media changes, so that policy-makers better understand how new and emerging capabilities might affect DoD and its personnel.

(2) Develop DoD-wide education and more clearly state training requirements that cover social media and mobile technologies.

(3) Develop and implement mandatory Defense Information Systems Agency's (DISA) Information Assurance Support Environment training program related to the security risks and vulnerabilities of mobile apps.

(4) Update the DoD's and the Services' social media guidance on an annual or bi-annual basis so that it addresses the most current technologies and platforms. Furthermore, the Services should develop additional means for disseminating this guidance to ensure that Service members are aware of, and acting in compliance with, this guidance.

[27] An early version of this report was shared with representatives from the office of the DoD CIO who responded to the recommendations resulting in updates to the final version of the report.

# REFERENCES

460th Space Wing Public Affairs. (2013). *DoD warns of non-sanctioned MyPay app.* Retrieved from http://www.afspc.af.mil/news1/story.asp?id=123366577

Adler, E. (2014). *Social media engagement: The surprising facts about how much time people spend on the major social networks*. Retrieved from http://www.businessinsider.com/social-media-engagement-statistics-2013-12

Alter, M., & Riva, C. (2014). *9 creepy apps to watch out for: Swarm, Stalker, Crush, Wingman, NameTag, Breakup, Girls Around Me*. Retrieved from http://www.newsnet5.com/news/9-creepy-apps-to-watch-out-for-swarm-stalker-crush-wingman-nametag-breakup-girls-around-me

Associated Press. (2007). *Soldiers face punishment over blogs*. Retrieved from http://www.military.com/NewsContent/0,13319,134461,00.html

Bessette, C. (2014). *What's the difference between Whisper and Secret*? Retrieved from http://tech.fortune.cnn.com/2014/04/04/whats-the-difference-between-whisper-and-secret/

Bowles, N. (2014). *Whisper launches mental health nonprofit*. Retrieved from http://recode.net/2014/08/14/whisper-launches-nonprofit-for-suicide-prevention/

Brenner, J., & Smith, A. (2013). *72% of online adults are social networking site users*. Retrieved from http://pewInternet.org/Reports/2013/social-networking-websites/Findings.aspx

Buck, S. (2012). *10 things you can fit into your 63,206-character Facebook status.* Retrieved from http://mashable.com/2012/01/04/facebook-character-limit/

CIO Council. (2013). *Privacy best practices for social media*. Retrieved from https://cio.gov/wp-content/uploads/downloads/2013/07/Privacy-Best-Practices-for-Social-Media.pdf

Clark, J. F. (n.d.). *History of mobile applications*. Retrieved from http://www.uky.edu/~jclark/mas490apps/History%20of%20Mobile%20Apps.pdf

Coldewey, D. (2014). *Mobile app use doubles, social apps triple in 2013: Report.* Retrieved from http://www.nbcnews.com/technology/mobile-app-use-doubles-social-apps-triple-2013-report-2D11917954#

Datoo, S. (2014) *You can now chat and have live video conversations with your friends on Snapchat.* Retrieved from http://www.buzzfeed.com/sirajdatoo/you-can-now-chat-and-have-live-video-conversations-with-your

## REFERENCES

Defense Finance and Accounting Service. (2013). *DFAS 'Info2Go' app available in the Apple App Store and the Android market*. Retrieved from http://www.dfas.mil/pressroom/dfasnewsreleasearchive/Release1312002.html

Dellinger, A. J. (2014). *We try hiding our secrets with "Confide," the Snapchat of text and emailing*. Retrieved from http://www.digitaltrends.com/mobile/confide-app-review/

Department of Defense Directive 1344.10. (2008). *Political activities by members of the Armed Forces*.

Department of Defense Instruction 1325.06. (2012). *Handling dissident and protest activities among members of the Armed Forces.*

Department of Defense Instruction 8550.01. (2012). *DoD Internet services & Internet-based capabilities*.

Department of Homeland Security. (2010). *Terrorists use of social networking Facebook case study*. Retrieved from http://publicintelligence.net/ufouoles-dhs-terrorist-use-of-social-networking-facebook-case-study/

Doll, J. (2012). *Al Qaeda wants to be your friend on Facebook*. Retrieved from http://blogs.villagevoice.com/runninscared/2012/01/al_qaeda_wants_to_be_your_facebook_friend.php

Ewing, P. (2010). *Monitors: Jihadist threat to Navy increasing*. Retrieved from http://www.navytimes.com/article/20100106/NEWS/1060333/Monitors-Jihadist-threats-Navy-increasing on May 14, 2014.

Facebook. (2011). *From A to YouTube…22 terms to help navigate the social media maze*. Retrieved from https://www.facebook.com/notes/discover-network/from-a-to-youtube-22-terms-to-help-navigate-the-social-media-maze/303151316376389?ref=nf

Facebook. (n.d.). *What are social plugins*. Retrieved from https://www.facebook.com/help/103828869708800

Fance, C. (2012). *6 great plugins for adding a social stream to your blog*. Retrieved from https://managewp.com/social-stream-plugins

Federal Trade Commission. (2014). *Snapchat settles FTC charges that promises of disappearing messages were false*. Retrieved from http://www.ftc.gov/news-events/press-releases/2014/05/snapchat-settles-ftc-charges-promises-disappearing-messages-were

Fingleton, E. (2012). *The Petraeus affair and the risk of blackmail: Another nail in America's coffin*. Retrieved from http://www.forbes.com/sites/eamonnfingleton/2012/11/10/the-petraeus-affair-another-nail-in-americas-coffin/

Fitzpatrick, P. (2014). *Connecting military families with social media*. Retrieved from http://www.huffingtonpost.com/peg-fitzpatrick/connecting-military-famil_b_4670683.html

Gannes, L. (2013). *Why should you care about whisper, the secret-sharing app that VCs are pouring money into*? Retrieved from http://allthingsd.com/20130905/why-should-you-care-about-whisper-the-secret-sharing-app-that-vcs-are-pouring-money-into/

Gaudin, S. (2010). *Social networks leak your information, study says*. Retrieved from http://www.computerworld.com/s/article/9178648/Social_networks_leak_your_information_study_says

GirlsAround.me. (n.d.). *Girls Around Me*. Retrieved from http://girlsaround.me/

Google. (n.d.). *Malware*. Retrieved from https://www.google.com/search?q=define+malware&sourceid=ie7&rls=com.microsoft:en-us:IE-Address&ie=&oe=

Heggestuen, J. (2013). *One in every 5 people in the world own a smartphone, one in every 17 own a tablet*. Retrieved from http://www.businessinsider.com/smartphone-and-tablet-penetration-2013-10

Identity Theft Resource Center. (2013). *Risks of mobile applications*. Retrieved from http://www.idtheftcenter.org/Cybersecurity/risks-of-mobile-applications.html

Jones, P. (2012). *Military social media mishaps*. Retrieved from http://www.dreamgrow.com/military-social-media-mishaps/

Kellogg, K. (2013). *What is Klout? What is Kred? 3 Ways to wield social influence scores for improved online interactions*. Retrieved from http://www.bruceclay.com/blog/2013/11/what-is-klout/

Khalaf, S. (2014). *Mobile use grows 115% in 2013, propelled by messaging apps*. Retrieved from http://blog.flurry.com/bid/103601/Mobile-Use-Grows-115-in-2013-Propelled-by-Messaging-Apps

Koren, M. (2014) *Iranian hackers target U.S. military officials with elaborate social media scam*. Retrieved from http://www.defenseone.com/technology/2014/05/iranian-hackers-target-us-military-officials-elaborate-social-media-scam/85417/.

Kramer, N.C. & Haferkamp, N. (2011). *Privacy online: Perspectives on privacy and self-disclosure in the social* web. Chapter 10 (*Online self-presentation: Balancing privacy concerns and impression construction on social networking sites*), pp. 127-141. Springer Heidelberg Dordrecht, New York, NY.

## REFERENCES

Leccese, C., and Seligman, M. (2013). *Social media's unique relationship with military families*. Retrieved from https://www.militarymentalhealth.org/blog/2013/12/social-medias-unique-relationship-with-military-families/

Likmeta, B. (2014). *Al Qaeda's using social media to find new recruits in Europe*. Retrieved from http://www.globalpost.com/dispatch/news/regions/europe/140123/albania-isis-al-qaeda-social-media-europe

Lister, J. (2012). *Facebook scam dupes military, gov't officials*. Retrieved from http://www.infopackets.com/news/7328/facebook-scam-dupes-military-govt-officials

Luckerson, V. (2013). *The new war in mobile is all about messaging apps like Snapchat*. Retrieved from http://business.time.com/2013/12/13/the-new-war-in-mobile-is-all-about-messaging-apps-like-snap-chat/

Madden, M. (2012). *Privacy management on social media sites*. Retrieved from http://www.pewInternet.org/files/old-media/Files/Reports/2012/PIP_Privacy_management_on_social_media_sites_022412.pdf

Madejski, M., Johnson, M., & Bellovin, S.M. (2012). *A study of privacy setting errors in an online social network*. Retrieved from http://maritzajohnson.com/publications/2012-sesoc.pdf

Marsden, P. (2009). *Simple definition of social commerce*. Retrieved from http://digitalintelligencetoday.com/social-commerce-definition-word-cloud-definitive-definition-list/

Militaryhandbooks.com. (2013). *Identity theft scam with TSP mobile phone app*. Retrieved from http://militaryhandbooks.com/identity-theft-scam-with-tsp-mobile-phone-app/

National Security Agency. (n.d.). *Intelligence collection activities and disciplines.* Retrieved from http://www.fas.org/irp/nsa/ioss/threat96/part02.htm

Nielsen. (2014). *The U.S. digital consumer report*. Retrieved from http://www.nielsen.com/us/en/reports/2014/the-us-digital-consumer-report.html

O'Reilly, T. & Battelle, J. (2009). *Web squared: Web 2.0 five years on.* Special Report. O'Reilly Media, Inc. Retrieved from http://gossgrove.com/sites/default/files/web2009_websquared-whitepaper.pdf

PCMag.com. (n.d.). *Encyclopedia: Definition of: mobile app*. Retrieved from http://www.pcmag.com/encyclopedia/term/60015/mobile-app.

PCMag.com. (n.d.). *Encyclopedia: Definition of: smartphone*. Retrieved from http://www.pcmag.com/encyclopedia/term/51537/smartphone

Proskauer Rose LLP. (2014). *Social media in the workplace around the world 3.0.* Retrieved from http://www.proskauer.com/files/uploads/social-media-in-the-workplace-2014.pdf

Rainie, L., Kiesler, S., Kang, R., & Madden, M. (2013). *Anonymity, privacy, and security online*. Retrieved from http://pewInternet.org/Reports/2013/Anonymity-online.aspx

Rock. M. (2013). *Facebook wants favor in Washington for adding jobs*. Retrieved from http://www.mobiledia.com/news/108863.html

Rodewig, C. (2012). *Geotagging poses security risks*. Retrieved from http://www.army.mil/article/75165/Geotagging_poses_security_risks/

Ronca, D. (n.d.). *Top 5 niche social networks*. Retrieved from http://computer.howstuffworks.com/Internet/social-networking/information/5-niche-social-networks.htm

Rushe, D. (2014) *WhatsApp: Facebook acquires messaging service in $19bn deal.* Retrieved from http://www.theguardian.com/technology/2014/feb/19/facebook-buys-whatsapp-16bn-deal

Shepard, M. (2013). *Terror groups turn to Twitter, Facebook, YouTube to gain support, analysts say*. Retrieved from http://www.thestar.com/news/world/2013/02/14/terror_groups_turn_to_twitter_facebook_youtube_to_gain_support_analysts_say.html

Smith, C. (2013). *New app scam targets military personnel*. Retrieved from http://www.wtvm.com/story/23909281/new-app-scam-targets-military-personnel

Social Media Today. (2013). *Increased presence of terrorist organizations on social media: Challenges for social networks*. Retrieved from http://socialmediatoday.com/prasant-naidu/1786511/terrorist-organizations-social-media-challenges-social-networks

Solis, B. & Thomas, J. (2013). *You are at the center of the Conversation Prism.* Retrieved from http://www.briansolis.com/2013/07/you-are-at-the-center-of-the-conversation-prism/

Surowiecki, J. (2005). *The wisdom of crowds.* Anchor Books. New York, NY.

The Week. (2012). *Are terrorists posing as hot girls on Facebook to spy on soldiers*? Retrieved from http://theweek.com/article/index/233114/are-terrorists-posing-as-hot-girls-on-facebook-to-spy-on-soldiers

United States Air Force. (2012). *Navigating the social network: The Air Force guide to effective social media use.* Washington, DC: Department of the Air Force.

## REFERENCES

United States Air Force. (2013). *Air Force social media guide*. Washington, DC: Department of the Air Force.

United States Army. (2013). *The United States Army social media handbook version 3.1.* Washington, DC: Department of the Army.

United States Navy. (2010). *ALNAV 057/10* (unofficial Internet post). Retrieved from http://www.public.navy.mil/bupers-npc/reference/messages/Documents/ALNAVS/ALN2010/ALN10057.txt

United States Navy. (2012). *Navy command leadership social media handbook*. Washington, DC: Department of the Navy.

Utz, S. & Kramer, N.C. (2009). The privacy paradox on social network sites revisited: The role of individual characteristics and group norms. *Cyberpsychology: Journal of Psychosocial Research in Cyberspace*, 3(2), article 1.

Vaas, L. (2014). *Stalker-friendly app, NameTag, uses facial recognition to look you up online*. Retrieved from http://nakedsecurity.sophos.com/2014/01/09/stalker-friendly-app-nametag-uses-facial-recognition-to-look-you-up-online/

Westerholm, R. (2013). *Ohio University student charged with four felonies in Snapchat sex extortion scam*. Retrieved from http://www.universityherald.com/articles/6514/20131230/ohio-university-student-charged-with-four-felonies-in-snapchat-sex-extortion-scam.htm

Wolcott, M. (2007). *What is web 2.0*? Retrieved from http://www.cbsnews.com/news/what-is-web-20/

Zhang, M. (2012). *US Army warns soldiers that pictures can kill*. Retrieved from http://petapixel.com/2012/03/21/us-army-warns-soldiers-that-geotagged-photos-can-kill/

Zimmerman, N. (2014). What PTSD is actually like according to real military veterans. Retrieved from http://www.buzzfeed.com/neetzanzimmerman/what-ptsd-is-actually-like-according-to-veterans

# APPENDIX A:

# GLOSSARY[28]

[28] Sources for Glossary entries include: The United States Army *Social Media Handbook Version 3.1*, released January 2013; the Air Force's *Navigating the Social Network*, released March 2012; Facebook; Wikipedia; Mashable; social media websites' "About" pages; mobile application descriptions in the Apple App Store and PCMag.com.

- Angie's List: Founded by Angie Hicks in 1995, Angie's List is an advertising website containing local business reviews. It has approximately 2-2.5 million paid members.
- Apple App Store: The Apple App Store is a digital platform for distributing mobile apps on the iOS (Apple) operating system. Users are able to browse and download apps directly to their iOS device (e.g., iPhones and iPads). The Apple App Store is maintained by Apple, Inc.
- App scams: Developed by malicious actors, these apps are intended to access users' smartphone systems to access stored information which can include credit card and account numbers, as well as logins, passwords, calendars, etc.
- App.net: An ad-free online social networking service and microblogging service that allows users to write messages up to 256 characters. Also allows applications to attach arbitrary metadata to posts.
- BazaarVoice: A website where users can view and share opinions, questions, and experiences about 20 million products in the BazaarVoice network.
- Blogs: An abbreviation of "Web log," blogs are websites with dated items of content in reverse chronological order that are self-published by an individual. Posts are typically about a particular subject, are usually available as feeds, and often allow commenting.
- Buzzfeed: BuzzFeed is a social news website that uses content-driven publishing technology to present users with popular news stories, videos, quizzes, and entertainment. Users can create their own profile and post their own articles in the community section of the website; the company also has a staff of writers.
- Chatter: An enterprise social networking website that allows employees, customers, and suppliers to join the network to communicate with relevant users.
- Classmates: A social networking website designed to help high school and college classmates reconnect.
- Confide: An Apple Inc. messaging application combining end-to-end encryption with "screenshot-proof" messages that disappear after they are read, facilitating confidential messaging.
- Content: Text, pictures, videos, and any other meaningful material that is on the Internet.
- Crowd Wisdom: Websites that use crowdsourcing to develop the content of the website and highlight the content based on popularity. Crowdsourcing is when ideas and content are submitted by the community to generate popular entertainment and news.
- Crowdsourcing: Websites that harness the skills and enthusiasm of those outside an organization who are prepared to volunteer their time contributing content and solving problems.

- Crowdspring: On online marketplace for crowdsourced creative services. Companies that need custom website designs, logos, graphic designs, or copywriting post ads describing the service they need, when they need it, and how much they will pay for this service. Users respond by submitting their work and companies choose the design or effort from the work submitted.
- Curation: Collecting, filtering, reviewing, and sometimes providing commentary on articles, images, and videos. Curation does not include creating new content on social media, but reviewing and reposting something that another user originally posted.
- Data Aggregator: An organization that compiles information from databases on individuals and sells the information to others.
- Digg: A social news website that allows members to submit and vote for articles. Articles with the most votes appear on the homepage of the site and subsequently are seen by the largest portion of the site's membership as well as other visitors.
- Discussions and Forums: An online discussion site (also known as a message board). Allows users to post and receive questions and messages.
- Disqus: A blog comment-hosting service for websites and online communities that use a networked platform. The service provides features such as social integration, social networking, user profiles, moderation tools, and analytics.
- Docstoc: A website for small business owners. It provides users with a selection of professional documents (e.g., day laborer contract, payment agreement, and waiver of service) and other resources like instructional videos, articles, and productivity tools.
- Elance: A social networking website designed to connect freelance workers with job opportunities.
- Evernote: A mobile app allowing users to take notes, save photographs, create to-do lists, and record voice reminders.
- Facebook: A social networking website. Users can create a personal profile, add other users as friends, and exchange messages and profile updates.
- Flickr: A social network centered around online photo sharing. The service allows users to store photos online and then share them with others through profiles, groups, and other methods.
- Foursquare: A location-based social networking website, software for mobile devices, and also a game. Users "check-in" at venues using a mobile website, text messaging or a device-specific application — they are then awarded points and sometimes "badges" for frequent visits.
- "Friend:" Another social media user with whom an individual connects and allows to view his/her profile. Users must request to be someone's friend and then must be accepted by the user.

- Geotagging: The act of embedding geographical data into photos, videos, and other files. Information appears as a file’s metadata. People may also geotag their whereabouts.
- Google+: A social networking service operated by Google Inc. The service launched on June 28, 2011, in an invite-only “field testing” phase.
- Google Groups: Online discussion forums that users can create and join, and are connected to Gmail and Google + accounts.
- Google Play Store: Originally the “Android Market,” the Play Store is a digital platform for distributing applications and digital media. The Play Store was developed by Google.
- Groupon: A website where users can purchase discounted gift certificates for a specific product or service from local and national companies. Companies included on the website include, but are not limited to, restaurants, gyms, day spas, mechanics, and hotels.
- Groups: Collections of individuals with some sense of unity through their activities, interests, or values. They differ from networks, which are dispersed, and defined by nodes and connections.
- Influence: Platforms that measure the extent to which people online are paying attention and responding to a particular user or brand (Kellogg, 2013).
- Insecure apps: Apps that were not developed using appropriate software security techniques that protect against common exploits.
- Instagram: A social network where users share photographs and videos. Users can connect their Instagram accounts to other social media websites like Facebook.
- iOS: Formerly iPhone Operating System, iOS is a mobile operating system developed by Apple Inc. iOS is the operating system powering the iPhone, iPad, and a host of other Apple products.
- Kickstarter: A website where users donate money to help fund creative projects posted by others.
- Klout: A website that assigns a number using social media analytics to each user from 1-100, which is a reflection of his/her social influence online.
- Kred: A website that assigns two numbers to each user based on two values: (1) influence and (2) outreach. The influence score refers to the users’ ability to inspire action; outreach refers to the user’s engagement with other social media users and whether they help spread a message. Both scores are calculated using Twitter and Facebook behavior.
- Like: An action that can be made by a Facebook user. Instead of writing a comment for a message or a status update, a Facebook user can click the “Like” button as a quick way to show approval and share the message.
- LinkedIn: A business-oriented social networking site.

- Livecasting: Broadcasting real-time video feed to an audience accessing the video stream over the Internet.
- LivingSocial: A website where users can purchase discounted gift certificates for a specific product or services from local and national companies. Companies included on the website include, but are not limited to, restaurants, gyms, day spas, and hotels.
- Location social media: Users submit location data for the purposes of interacting relative to their location.
- Malware: Software that is designed to damage or disable computer systems.
- Mashable: Founded by Pete Cashmore in 2005, Mashable is a news website, technology, and social media blog.
- Messaging Apps: Mobile applications that allow users to exchange written and visual messages.
- Metadata: Data that provides information about one or more aspects of content.
- Microblog: Social media site, such as Twitter, that allows users to share small elements of information such as short sentences, individual images, video and website links.
- milBook Webmasters: A group on milBook, an online collaboration tool that is a component of milSuite. MilSuite is a collection of online apps the mirror existing social media platforms and are focused on secure collaborations between DoD personnel.
- Mobile application or app: Software designed to run on a mobile device, like a smartphone. Designed to quickly access information, games, tools and other helpful programs.
- Name Tag: Name Tag is a facial recognition app that can be used to match a picture to an established social media profile or other online content associated with a specific person. For example, a Name Tag user can take a picture of a person on the street and the app will attempt to match the face to publicly available content (e.g., Facebook, Match.com, and possibly criminal or sex offender registries).
- News Feed: A feature of users' Facebook accounts. It provides constant updates of the people and pages followed on Facebook; can include status updates, photos, videos, links, and app activity.
- Nicheworking: "A social network that targets a select segment of the population…allows users to connect with fewer people who have the same interests, hobbies, or professional associations" (Ronca, n.d.).
- Nike+ Running: A mobile application that tracks users' distance and running speed.
- Pandora: A social online radio station that allows users to create stations based on their favorite artists and types of music.

- Photo Sharing: Uploading images (for public consumption) to a website like Flickr, adding tags and offering users the opportunity to comment or even re-use photos if users add an appropriate copyright license.
- Pinterest: A website and mobile application where users create, organize, and share visual bookmarks on their homepage.
- Plancast: A website where users can plan, promote, or find out about social activities in their neighborhood.
- Privacy Settings: Options offered by each social media platform to allow users to control who can and cannot see their profile.
- Profiles: Information that users provide about themselves when signing up for a social networking site as well as a picture and basic information. This may include personal and business interests, and a "blurb" and tags to help users search for like-minded people.
- Q&A: Question and answer websites. Content is controlled by its users.
- Quantified Self: Self-knowledge through tracking all aspects of one's daily life (e.g., number of steps walked, calories consumed, blood oxygen levels, heart rate at various times and environments, etc.).
- Quora: A question and answer-based website with blog capabilities. It advertises that users' questions are answered by individuals with first-hand experience.
- Ravelry: A social media website focused on fiber arts, like knitting, crocheting, spinning, and weaving.
- Secret: An Apple app allowing users to share messages anonymously within a circle of friends, friends of friends, or publicly.
- SlideShare: An online social network for sharing presentations and documents. Users can view files or embed them on other social networks.
- Smartphone: A mobile phone that can perform many of the same operations as a desktop computer.
- Snapchat: Allows users to capture and send images and videos with added text to other users. The sender can set a time limit for how long the receiver can view the image or video before the content is destroyed.
- SnapCapture: A mobile app for Android phones that saves unopened SnapChat images to the users' phone, thereby overwriting the self-destructive elements of SnapChat.
- Social Apps: Applications that allow users to communicate with other users.
- Social Bookmarks: An online service that allows users to collect, annotate and share bookmarked websites.
- Social Commerce: Ratings, reviews, social shopping, and user forums and communities.

- Social Marketplace: An online community that harnesses the power of social networks for the introduction, buying, and selling of products, services, and resources.
- Social Media: Tools and platforms people use to publish, converse, and share content online.
- Social Networks: An online service, platform, or site that focuses on facilitating the building of relationships between people who might share interests, activities, backgrounds, or real-life connections.
- Social Networking: Online places where users can create profiles and then socialize with others using a range of social media tools including blogs, video, images, tags, lists of friends, forums and messages.
- Social Streams: A stream of posts and updates from various social networks. Status updates and shared content like links, images, and videos can be displayed.
- Social web: A set of social relations that link people through the World Wide Web. It encompasses how websites and software are designed to support and encourage social interaction.
- Stream: Multimedia that is constantly received by, and presented to, users while being delivered by a provider.
- Tablet Computer: A mobile computer equipped with sensors, cameras, microphone, and touchscreen technology. A tablet computer can perform most of the same functions as a traditional desktop or laptop computer.
- TripAdvisor: A travel website that assists customers in gathering travel information, posting reviews and opinions of travel-related content, and engaging in interactive travel forums.
- Twitter: A platform that allows users to share 140-character-long messages publicly and privately to approved followers, depending on privacy settings. Users can “follow” each other as a way of subscribing to one another’s messages. Additionally, users can use the @username command to direct a message towards another Twitter user as well as send private messages.
- Tumblr: A microblogging platform that allows users to post text, photos, videos, links, quotes, and audio to their tumblelog, a short-form blog.
- User-generated Content: Content created by social media users.
- Ustream: A video streaming service that provides videos related to news, gaming, entertainment, sports, animals and wildlife, music, technology, and education.
- Video Sharing Website: allows users to upload, share, view, and comment on videos.

- Vimeo: A popular video-sharing service in which users can upload videos to be hosted online and shared and watched by others. Vimeo user videos are often more artistic, and the service does not allow commercial video content.
- Web 1.0: A term coined by O'Reilly Media in 2004 to describe websites where users were incapable of commenting, adding to, or revising posted material.
- Web 2.0: A term coined by O'Reilly Media in 2004 to describe blogs, wikis, social networking sites, and other Internet-based services that emphasize collaboration and sharing, rather than less interactive publishing (Web 1.0). It is associated with the idea of the Internet as a platform.
- Whisper: A social media app for iOS and Android enabling users to send and receive messages anonymously.
- Wiki: A website, with no defined leader, that allows users to edit its content.
- Wikipedia: An online encyclopedia created by thousands of contributors across the world.
- World Wide Web (www): The World Wide Web is a system of interlinked documents accessed through the Internet.
- Yammer: A professional social networking website and mobile application where employees and employers can share content, engage in online conversations, and share business data.
- YouTube: A video streaming website where users post and view videos.
- Zvents: Zvents is a network of social media websites that posts event details.

# APPENDIX B:

# MOBILE APPLICATIONS MARKETED TO THE DOD COMMUNITY

Not all apps that pose a threat to personal safety are easily identifiable. Table B-1 presents a short list of current apps available to the DoD community in the Google Play Store. Initially, it would be difficult for the average user to discern legitimate apps from those that are potentially harmful. Most of the apps in Table B-1 were developed by valid sources such as the DoD, the U.S. Army, a nonprofit group, or an educational institution, but some were released by unknown developers. For example, the MyPay Defense Finance and Accounting Service (DFAS) Leave and Earning Statement (LES) app is free in the Google Play Store and it allows users to connect to the DFAS to access MyPay accounts. From here users can update security questions, review accounts, and change passwords (460th Space Wing Public Affairs, 2013). It has been downloaded over 50,000 times but the app is not sponsored by any U.S. government agency (Smith, 2013). Consequently, users may be sharing their personal financial information with an unknown third party, and may be at risk for:

(1) Downloading malware: Software that is designed to damage or disable computer systems (Google, n.d.).

(2) App scams: Developed by malicious actors, these apps are intended to access users' smartphone systems to access stored information, which can include credit card and account numbers, as well as logins, passwords, calendars, etc.

(3) Insecure apps: Some apps available in the mobile marketplace were not developed using appropriate software security techniques that protect against exploitation. Insecure banking and shopping apps could expose personal and financial information that may be exploited by criminals.

Users do have means to protect their devices, including (but not limited to): (1) installing anti-virus software to protect against viruses and malware; (2) using back-up programs to enable users to save all mobile information to a secure back-up folder either on a hard drive or a virtual drive; and (3) conducting a Google search on the name of the app to potentially identify known problems associated with the app (Identity Theft Resource Center, 2013). However this information is not widely known. All social media platforms are vulnerable to both accidental and intentional misuse, and malicious actors can and will exploit user-generated content regardless of the website or app used.

## APPENDIX B

**Table B-1**
**Mobile Applications for Military Personnel and their Families**

| Mobile Applications Designed for Users in the Military Community | | |
|---|---|---|
| **App** | **Description** | **Designed for:** |
| Sesame Street for Military Families* | Bilingual mobile app designed to support children with issues like deployments, grief, and self-expression. | Military families |
| Call dibs* | Buy and sell goods within the military community. | Military community |
| Army OneSource Money Matters* | Financial tools to help families save and plan for the future. | Military personnel & families |
| DFAS Info2Go** | An official DoD app that allows access to MyPay features. | Military personnel & DoD civilians |
| MyPay DFAS LES* | Allows users to connect to the Defense Finance and Accounting Services to access MyPay account. This app is not sponsored by DoD or the U.S. government. | Military personnel & DoD civilians |
| TSP* | The Thrift Savings Plan (TSP) app allows users to access account information. This is not an official TSP app and TSP does not recommend using this app to access one's account (MilitaryHandbooks.com, 2013). | Military personnel & DoD civilians |
| Military and Money | App includes videos, articles, and tools to help people achieve financial freedom. Developed by McGraw Hill. | Military personnel & families |
| Military by Owner* | Allows users to preview homes on their iPhone. Users can search for a home by military base or current location. | Military personnel & spouses |

*Third party developers
**Currently the only DFAS-approved app available (DFAS, 2013).